



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,526	08/16/2001	Arindam Das-Purkayastha	B-4274 618998-3	3735

22879 7590 03/07/2006

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER

CHAI, LONGBIT

ART UNIT PAPER NUMBER

2131

DATE MAILED: 03/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/931,526

Applicant(s)

DAS-PURKAYASTHA ET AL.

Examiner

Longbit Chai

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 January 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-61 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-61 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 6 were originally received for consideration. New claims 7 – 61 were added in the amendment filed on December 14, 2004. The amendment filed have been entered and made of record. Presently, pending claims are 1 – 61.

Response to Arguments

2. Applicant's arguments filed on 1/13/2006 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, new grounds of rejection have been made – see the following Office action.

Claim Objections

3. Claim 42 is objected to because the following informalities: "comparing at the user values" is better to be presented as "comparing at the user the values" for clarity to avoid confusion with "comparing the user values". Appropriate correction is required. Any other claims not addressed are objected by virtue of their dependency should also be corrected.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

1. Claims 1, 6, 7, 24 and 42 are rejected under 35 U.S.C. 101 because the claimed subject matter is merely drawn to a collection of data fields – for example, the integrity metrics and the trust levels (e.g., level 1, 2 and so on) which are merely non-functional descriptive material and as such the claimed subject matter fails to produce the useful and tangible results. Any other claims not addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1 – 9, 11 – 19, 22 – 26, 28 – 37, 42 – 44, 46 – 55, 60 and 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Farber et al. (U.S. Patent 6415280), in view of Grawrock (U.S. Patent 6678833).

As per claim 42 (and claim 1, 6, 7 & 24), Farber teaches a method for establishing communications between a computer entity and a user, comprising:

comparing at the user the values in the integrity metric calculated for the entity by the trusted device (Farber: Column 34 Line 45 – 62, Column 12 Line 38 – 42: the True Name – i.e., the MD (Message Digest), signature / hash value, of a data block – is interpreted as the integrity metric); and

selecting at the user a level of trust for the entity from a plurality of predefined levels of trusts available to the user based on at least one value in the integrity metric calculated for the entity by the trusted device (Farber: Column 34 Line 45 – 62, Column 31 Line 27 – 36 and Column 23 Line 42 – 44: (a) the trusted party is considered as the network server, from the system perspective as a whole, along with the local processor / server that contains the True File Registry (b) the levels of trust are considered as, at least, trust or non-trust as the result of comparison determined by the system).

However, Farber does not disclose expressly the trusted device.

Grawrock teaches presenting a request from the user to a trusted device (Grawrock: Column 4 Line 9 – 11: the challenger is considered as the user and the TPM (Trusted Platform Module) is considered as the trusted device – i.e. any device resident at the trusted platform (TPM) is indeed a trusted device) associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity (Grawrock: Column 2 Line 5 – 6 and Column 4 Line 7 – 9: the hash value).

presenting to the user a response from the trusted device including an integrity metric calculated for the entity by the trusted device (Grawrock: Column 4 Line 9 – 10).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Grawrock within the system of Farber because (a) Farber teaches providing a resource integrity checking mechanism by validating the integrity metric stored at the remote trusted party and the one reported by the local processor (Farber: Column 34 Line 45 – 62) and (b) Grawrock teaches the integrity metric reported by the local processor should be carried out by the trusted device to ensure the reported data is indeed trustworthy without the reliance on any intervening devices (Grawrock: Column 2 Line 5 – 6).

As per claim 2, Farber as modified further teaches the trusted device is arranged to acquire an integrity metric of the computer entity (Grawrock: Column 3 Line 62 – Column 4 Line 9).

As per claim 3, Farber as modified teaches the trust level is determined by comparing the value of the at least one characteristics with a specified value (Farber: Column 34 Line 45 – 62).

As per claim 4, Farber as modified further teaches the plurality of trust levels are determined base upon a plurality of specified values associated with a plurality of characteristics of a computer entity (Grawrock: Column 4 Line 6 – 9).

As per claim 5, Farber as modified further teaches the plurality of trust levels are determined based upon a plurality of specified values associated with characteristics for a plurality of computer entities (Farber: Column 34 Line 45 – 62: (a) the plurality of trust levels are trust or non-trust (b) a plurality of specified values associated with characteristics for a plurality of computer entities are a plurality of hash (MD) values associated with a plurality of executable applications (Farber: Column 34 Line 50 – 51)).

As per claim 8, 11, 25, 28, 43 and 46, Farber as modified further teaches the trusted device is hardwired to the computer entity (Grawrock: Figure 2 and Column 3 Line 25 – 30).

As per claim 9, 26 and 44, Farber as modified further teaches the trusted device is configured to control the boot process of the computer entity (Grawrock: Column 3 Line 61 – 67).

As per claim 12, 29 and 47, Farber as modified further teaches the trusted device is configured to contain one or more of a public encryption key, a private encryption key, and one or more authenticated values provided for the entity integrity metric by the trusted party (Grawrock: Column 4 Line 15 – 18).

As per claim 13, 30 and 48, Farber as modified further teaches the trusted device is configured to calculate the integrity metric by generating a digest of BIOS instructions

Art Unit: 2131

in the BIOS memory of the entity (Grawrock: Column 3 Line 61 – 67 and Column 4 Line 7 – 9).

As per claim 14, 31 and 49, Farber as modified further teaches the trusted device is configured to calculate the integrity metric by measuring one or more values of configuration information regarding one or more components of the entity (Grawrock: Column 4 Line 1 – 9).

As per claim 15, 32, 36, 50 and 54, Farber as modified further teaches the components of the entity are selected from among the group of components comprising hardware components and software components (Grawrock: Column 4 Line 1 – 6).

As per claim 16, 33 and 51, Farber as modified further teaches wherein the components of the entity are selected from among the group of components comprising the BIOS, ROM, operating system loader, and operating system of the entity (Grawrock: Column 4 Line 3 – 6).

As per claim 17, 34 and 52, Farber as modified further teaches the configuration information measured for at least one of the components comprises one or more of certificate information, last update information, latest update version information, and previous update information (Grawrock: Column 4 Line 15 – 18).

As per claim 18, 35 and 53, Farber as modified further teaches the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components (Grawrock: Column 4 Line 1 – 9).

As per claim 19, 37 and 55, Farber as modified further teaches the response received from the trusted device includes the authenticated values provided by the trusted party (Grawrock: Column 4 Line 35 – 40).

As per claim 22 and 60, Farber as modified further teaches initiating data transfer to the entity in accordance with the selected trust level (Farber: Column 34 Line 54 – 66).

As per claim 23 and 61, Farber as modified further teaches initiating data transfer to the entity in accordance with the selected trust level comprises transferring no data (Farber: Column 34 Line 54 – 66: if the hash (MD) remains the same).

3. Claims 10, 27 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Farber et al. (U.S. Patent 6415280), in view of Grawrock (U.S. Patent 6678833), and in view of Saunders (Patent Number: 6209099).

As per claim 10, 27 and 45, Farber as modified does not disclose expressly the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device.

Saunders teaches the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device (Saunders: Figure 3 Element 28: no further response from the trusted device if the boot key is not entered and configured).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Saunders within the system of Farber as modified because (a) Farber teaches providing a resource integrity checking mechanism by validating the integrity metric stored at the remote trusted party and the one reported by the local processor (Farber: Column 34 Line 45 – 62) and (b) Saunders teaches the integrity metric reported by the local processor should be carried out by a secure cryptographic engine (Saunders: Abstract).

4. Claims 20, 21, 38 – 41 and 56 – 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Farber et al. (U.S. Patent 6415280), in view of Grawrock (U.S. Patent 6678833), and in view of Stoltz (Patent Number: 6615264).

As per claim 20, 38 and 56, Farber as modified does not disclose expressly generating a nonce to pass to the trusted device with the request.

Art Unit: 2131

Stoltz teaches generating a nonce to pass to the trusted device with the request (Stoltz: Column 17 Line 64 – 66 and Column 18 Line 1 – 5: nonce is a random number).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Stoltz within the system of Farber as modified because (a) Farber teaches providing a resource integrity checking mechanism by validating the integrity metric stored at the remote trusted party (network server) and the one reported by the local processor (Farber: Column 34 Line 45 – 62) and (b) Stoltz teaches a security enhanced method to authenticate the request for secure information in a client-server networking system (Stoltz: Column 3 Line 65 – Column 4 Line 2, Column 4 Line 9 – 12, Column 17 Line 64 – 66 and Column 18 Line 1 – 5).

As per claim 21, 39 and 57, Farber as modified further teaches the response from the trusted device includes the nonce received with the request (Stoltz: Column 18 Line 46 – 47).

As per claim 40 and 58, Farber as modified does not disclose expressly the request includes input data.

Stoltz teaches the request includes input data (Stoltz: Column 17 Line 64 – 66 and Column 18 Line 1 – 5: random number is included as part of the request). See the same rationale address above in rejection claim 20.

Art Unit: 2131

As per claim 41 and 59, Farber as modified teaches the response includes the input data processed with the private encryption key (Stoltz: Column 17 Line 64 – 66, Column 18 Line 1 – 5 and Column 2 Line 33 – 34: the request / response message is encrypted).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


LBC

Longbit Chai
Examiner
Art Unit 2131

CHRISTOPHER REVAK
PRIMARY EXAMINER


3/5/06